LA-UR 91-2164

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE A METHODOLOGY FOR PERFORMING COMPUTER SECURITY REVIEWS

LA-UR--91-2164

DE91 016080

AUTHOR(S) William J. Hunteman

MASTER

SUBMITTED TO 32nd Annual Meeting of the Institute of Nuclear Materials Management, New Orleans, Lousiana, July 28-31, 1991

DISCLAIMER

1991

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

A METHODOLOGY FOR PERFORMING COMPUTER SECURITY REVIEWS

W. J. Hunteman
Los Alamos National Laboratory
Los Alamos, NM 87545

ABSTRACT

DOE Order 5637.1, "Classified Computer Security," requires regular reviews of the computer security activities for an ADP system and for a site. Based on experiences gained in the Los Alamos computer security program through interactions with DOE facilities, we have developed a methodology to aid a site or security officer in performing a comprehensive computer security review. The methodology is designed to aid a reviewer in defining goals of the review (e.g., preparation for inspection), determining security requirements based on DOE policies, determining threats/vulnerabilities based on DOE and local threat guidance, and identifying critical system components to be reviewed. Application of the methodology will result in review procedures and checklists oriented to the review goals, the target system, and DOE policy requirements. The review methodology can be used to prepare for an audit or inspection and as a periodic self-check tool to determine the status of the computer security program for a site or specific ADP system.

I. INTRODUCTION

This computer security review methodology is based on the approach followed in the Computer Security Enhancement Review (CSER) program conducted by Los Alamos National Laboratory experts in computer security. The review methodology is designed to achieve the following objectives:

- assess the effectiveness of the site's computer security program,
- determine and improve compliance with established policies,
- aid in the development of site capabilities in conducting computer security reviews,

- promote increased awareness of computer system vulnerabilities, and
- provide technical support to computer security.

A basic concept in the methodology is the assumption that anything that can affect the integrity of a computer system or its ability to support the organization's mission is a security issue. The methodology described in this report can be applied to the following areas:

- computer security policies,
- computer security program management,
- hardware security,
- software security,
- telecommunications security,
- physical and environmental security,
- personnel security, and
- administrative or procedural security.

Use of the methodology will result in a complete review of the security posture of an organization and computer system. [Note: throughout the following discussion the term computer system is used to refer to both the traditional computer system and to a network of computer systems.]

The examples used throughout this discussion are drawn from the DOE environment and are intended only to illustrate the particular point being discussed. The examples should not be interpreted as being complete or reflecting the requirements for the DOE Classified Computer Security Program.

II. METHODOLOGY

The methodology begins with the determination of the security requirements that must be met for compliance with the policy statements. After the general security requirements are determined, the system components to be reviewed are identified and then the threats to the components are defined. After the system components and threats are determined, the system-specific protection criteria are derived from the requirements. When the protection criteria and system components have been defined, the review techniques (document reviews, demonstrations, testing, etc.) are selected for use in the review. The actual review is conducted using the specific protection criteria. Completion of the review causes an assessment of the results and

correction of identified deficiencies or acceptance of the risks. The computer security review methodology steps are shown in Table I.

TABLE I

Security requirements	Definition of the requirements for computer and information security.
System components	Identification of details of facilities, including computer hardware, operating systems, applications performing security functions, and essential information to be protected.
Threat determination	Identification of technically credible threats or attack scenarios.
Protection criteria	Definition of criteria describing the minimum acceptable deterrence or detection capabilities, timeliness of detection, and essential components to be protected.
Review techniques	Identification of appropriate analysis techniques oriented towards key system components.
Review	Performance of the computer security review.
Evaluation	Evaluation of the results of the review to develop a plan to correct any deficiencies identified during the review or accept the level of risk exposed during the review.
Deficiency correction	Assessment of the results and correction of identified deficiencies or acceptance of the risks.

For example, expanding the security requirements into protection criteria may indicate that some security requirements were misstated or omitted. In this situation, repeating the security requirements phase would be necessary to include the corrected or new information. Figure 1 depicts the general process of the review methodology.

III. SECURITY REQUIREMENTS

The process of determining the security requirements begins with identifying the basic security issues contained in all applicable policy documents. The basic policies are typically

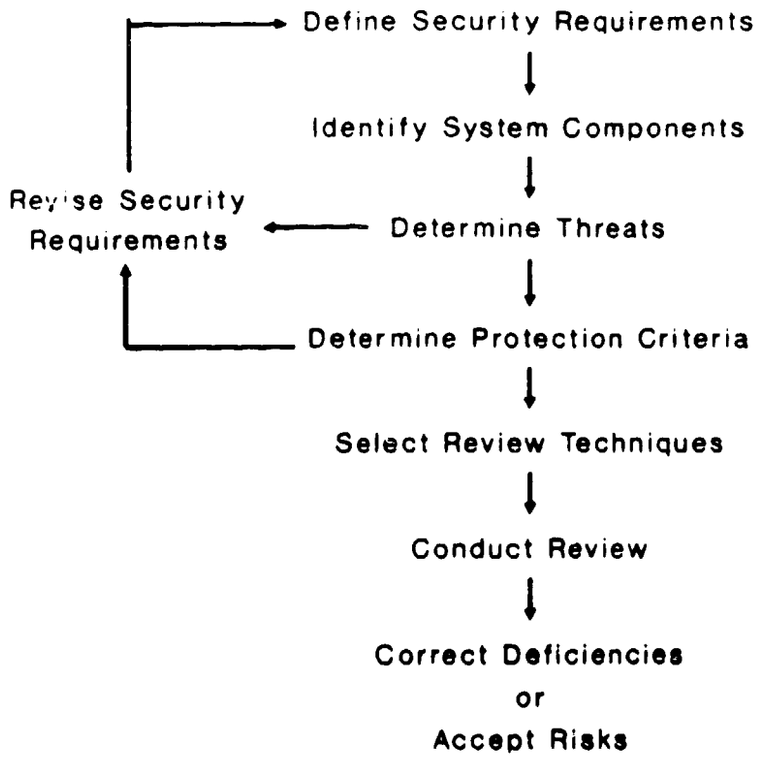

Fig. 1. Computer security methodology.

issued by an oversight organization, such as the DOE Office of Safeguards and Security. Other policy requirements may be found in the directives or orders issued by other organizations with responsibility for enforcement of the general policy. Another source of policy requirements may be site or corporate procedures for computer or information security.

During the identification of the basic requirements, any requirement contained in the documents referenced by any part of the computer security policy must be considered. After all policy requirements have been identified, each requirement should be expanded into one or more high-level requirements that apply to the systems to be reviewed. These requirements must be sufficiently specific that individual protection criteria can be identified to determine compliance with the policy.

Occasionally security specifications will exist for the computing systems to be reviewed. The security specifications should be reviewed for completeness and conformance with the appropriate policies. If the specifications are complete, they

should be used as the security requirements for the review. If the specifications are incomplete or do not conform to the policies, the security requirements should be developed from the various policies and guidelines, and the specifications should be included as part of the system components being reviewed.

For example, the DOE classified computer security policy, DOE 5637.1, includes deterrence from, or detection of, unauthorized access (disclosure), modification, destruction, and denial of use of computer hardware, software, and information. These basic issues can be further expanded into high-level requirements. Typical high-level requirements for a system in the DOE might be as follows:

- Deter (or detect) attempts by site or outside personnel to gain unauthorized access to computer hardware and software;
- Deter (or detect) unauthorized attempts by site or outside personnel to modify computer hardware, software, and information;
- Deter (or detect) unauthorized attempts by site or outside personnel to destroy any computer hardware, software, and information;
- Deter (or detect) any attempts by site or outside personnel to misuse the computer hardware, software, or information with the intent to deny the legitimate use of the resource.

These high-level requirements must be expanded into more detailed requirements to allow the determination of the necessary protection requirements. For example, the high-level requirement to deter (or detect) attempts by site or outside personnel to gain unauthorized access to computer hardware and software can be expanded into several specific requirements. Some of the specific requirements might be

- restricting file access to authorized users,
- requiring explicit authorization for users to access a file, and
- requiring authentication of all users before allowing access to the system.

These requirements will allow the identification of specific protection criteria for evidence that the policy is satisfied.

IV. IDENTIFICATION OF SYSTEM COMPONENTS

An essential part of the review preparation is identifying the system components to be reviewed, including computer hardware, operating systems, and applications that perform a security function. The identification typically begins with a general statement of the systems or area to be reviewed. The general statement is then expanded into more specific statements that identify specific system components until the personnel involved in the review (site personnel and the review team) are assured that the selected components will yield an accurate view of the security posture of the systems or area.

Depending upon the scope of the review, the system components may include elements of the areas of physical security, personnel security, telecommunications security, and hardware/software security.

V. THREAT DETERMINATION

The threats identified for the area or systems to be reviewed provide the basis for determining the protection criteria that must be implemented in the system to provide adequate protection for the classified information. The threats also provide a basis for evaluating the review results to determine if corrective action is needed or if the level of risk is at an acceptable level.

The identified threats for the area or systems being reviewed should be based on guidance from the policy and oversight organizations. The threats identified by the facility should be documented. The threat determination should also consider the probable goals and perspective of possible attackers. The scenarios should consider the resources necessary or available to the attacker, including any special computer knowledge. For example, an attacker motivated by ideology would use scenarios considerably different from attackers motivated by greed or desire to embarrass the facility. Including the attack scenarios in the threat determination will help ensure that all realistic threats are considered.

The DOE has issued a generic threat statement, "Department of Energy Generic Statement of Threat Against Classified Computing Resources and Classified Information," that provides basic guidance for identifying system-specific threats. Each site is required by DOE 5637.1 to prepare a site

Statement of Threat for Classified Computers that must incorporate the DOE generic statement and any other guidance issued by DOE organizations regarding threats to computer resources processing classified information. Each computer system processing classified information must also have a written statement of threat based on the site Statement of Threat. The system statement may be a simple acknowledgement that there are no additional statements of threat beyond those identified in the site statement.

VI. PROTECTION CRITERIA

Once the security requirements, system components, and threats have been defined, the criteria necessary for implementing the policy requirements can be identified. These criteria are the explicit mechanisms used to protect the information being processed by the computing resource. These protection criteria form the foundation of the entire review process. A review of the implementation of each of the protection mechanisms will yield a comprehensive assessment of the degree of protection provided by the system. Because the protection criteria are derived from policy requirements, the review will also produce a measure of system compliance with the policies.

Often the policy statements will be accompanied by guidelines or other statements of protection criteria. Regardless of the degree of detail in policy statements or guidelines, each of the security requirements should be expanded into one or more explicit protection criteria. Each of the protection criteria must define the minimum detection or deterrence capability, the required timeliness of detection (if appropriate), and the essential hardware, software, or information being protected. If the policy or guidelines are very detailed, the expansion may be unnecessary.

The identification of protection criteria must include, but may not be limited to, the policy statements. The computer security community has developed a wide range of generic criteria that may be used to identify additional protection criteria. These generic criteria have been developed by the US government and the European computer security community.

For example, if the high-level requirement is to deter (or detect) attempts by site or outside personnel to gain unauthorized

access to computer hardware and software, then some of its specific requirements could be as follows:

- file access must be restricted to authorized users,
- users must receive explicit authorization to access a file, and
- all users must be authenticated before given access to the system.

These requirements can be expanded into detailed protection criteria. For example, "all users must be authenticated before given access to the system" can be expanded into

- Users must be identified and authenticated as part of the process of accessing, i.e., logging onto the system,
- Procedures for distributing and protecting authentication materials must be established,
- Authorization for system access must be reviewed before access is granted,
- Authentication procedures must be periodically reviewed, and
- If passwords are used as the primary means of user authentication, then
  - Passwords must be machine generated,
  - The password generation algorithm must be documented and approved,
  - Passwords must be changed at least annually,
  - Passwords must be immediately changed if they are considered or actually are compromised, and
  - Methods used to protect the password files on the system must be documented and approved.

After the general protection criteria have been defined, each item should be rewritten or modified into a statement that applies to the actual systems being reviewed.

VII. SELECT REVIEW TECHNIQUES

After the system components and protection criteria are determined, the review team, with the cooperation of the site personnel, must select the techniques for reviewing the criteria. The review team chooses techniques based on their skills, the

time available for the review, protection criteria, system components to be protected, and likely threats to the systems.

The techniques must also consider the scope of the review. If the review is intended to assess compliance with established policy, the techniques used may differ significantly from a review intended to discover deficiencies in the implementation of protection criteria. For example, a compliance review might be limited to an exhaustive review of documentation (security plans, procedures, etc.) and a performance review might concentrate on hands-on testing by the review team.

The review techniques can be grouped into the categories of review of documentation (including evidence in logs), interviews, demonstrations, performance tests, and noncompliance tests (black-hat testing).

A. Review of Documentation

The review of documentation techniques are the heart of any review, and some review of documentation must be included in every computer security review. The information extracted during the review of documentation will improve the review team's understanding of the facility and establish a basis for verifying information obtained during the remainder of the review. Documentation review techniques may range from quickly reading the security plans for the systems to a detailed reading of all documentation related to the security posture of the facility or systems. If an in-depth approach is selected, then the documentation review should begin with the security plan for the system. The security plan should be reviewed for compliance with all established policies, including any local guidance on preparation of security plans. If the local guidance differs significantly from the general policies, then documentation of the authorization to deviate from the general policy must be identified and reviewed.

Documents to be reviewed should include security plans for each of the systems being reviewed, system contingency plans, all computer and information security procedures for the systems being reviewed, all site procedures for computer or information security, and any document incorporated by reference into any of these documents. The documents should be reviewed for compliance with established policies and evidence that the documents are being reviewed and updated regularly. Maintenance of the documents will be shown by files or logs of

review activities and changes. Further evidence of document maintenance may be obtained during interviews.

Other documents that should be considered for review include operations logs; hardware and software maintenance records; audit log reviews; reviews for waste, fraud, and abuse; training records; visitor access logs; authorization records; and sanitization and destruction logs.

Although a documentation review will provide a perspective on the status and history of the reviewed systems, the documentation must be confirmed by some other form of review technique. It is essential that the documentation accurately reflect the working status of the systems.

B. Interviews

Any review will involve at least some interviews with personnel at the facility. The interviews are critical to validate information obtained during the documentation review and to improve the review team's understanding of the facility operations. Ideally interviews should be conducted with personnel from all levels of the organization. The intent of the interviews should be to determine if the policies and management directives are communicated and implemented, and if the systems actually operate as described in the documentation.

The interviews may be either formal or just discussions during other review activities. During the interview the review team should be open and honest and avoid misleading questions. The reviewer must be certain that the interviewees understand the question before they respond. A useful technique is to always have two members of the review team present with one person asking the questions and the other documenting the questions and responses.

A useful technique during interviews is to ask one person or group how other individuals or groups perform (for example, ask a security officer how long it takes to get a security plan approved). The information should be validated by interviews with the other person or group. Another useful interview technique is to ask questions that require the interviewee to respond with more than a yes or no. For example, the review team might ask, "Is this the normal procedure?" followed by, "Have you been trained in this procedure?"

C. Demonstrations

Demonstrations and tours provide an opportunity for the review team to place the information collected during the documentation reviews and briefings into perspective, observe the environment that affects the operation of the systems, and collect considerable information about the operational practices. The demonstrations and tours should be scheduled to lessen the impact on system operations and be scheduled during normal operating hours.

Demonstrations and tours should be conducted by operators or personnel who normally work in the area rather than a supervisor or security personnel. Demonstrations conducted by operators will provide insight into actual operating practices and free the supervisor or security personnel for explanation or discussions of any significant events during the demonstration.

Information collected during a demonstration or tour should be validated by reviewing documentation, interviews, or performance testing because the demonstrations provide a controlled method for the facility personnel to illustrate how they believe the system is operating under normal operating conditions. Although the demonstrations may show correct operation of security features, the demonstration may not thoroughly exercise the security features and system being demonstrated.

D. Performance Tests

Performance tests are activities that allow the testing of a security feature or procedure under controlled conditions. The tests can involve any combination of computer equipment, site personnel, or operating procedures. Performance tests involving personnel are intended to review the effectiveness of the procedures and personnel knowledge and implementation of the procedures.

Performance tests must always be coordinated with facility personnel. Tests involving personnel will require that the affected personnel not be aware that the test is being conducted; however, facility personnel coordinating the review must be informed of the test activity. Some performance tests may require coordination with other facility personnel, such as the protective force, if the test could result in alarms or other notifications to the personnel.

The ideal performance test creates an environment that simulates realistic conditions that can be used to stress the security feature. The test should be designed to produce conclusive results for evaluating the effectiveness of the security feature. The efforts to create a realistic test environment and stress conditions must be balanced with the resources available to the review team, the site resources available for the test, and the test impact on normal operations. Performance testing should be designed to test a specific part of the system only if the review team has been requested to do so (or has identified a potential weakness). Normal performance testing should be comprehensive and address all major components of the system. Representative components can be tested and the results considered indicative of the entire system. For example, if a system contains several terminals, testing would be necessary only for a few (perhaps one or two) of the terminals.

Some performance testing should occur during every review to validate the information obtained from document reviews and interviews. More extensive performance testing should occur when requested by site personnel or when the review team suspects that the system may not be functioning as described in the documentation and interviews.

E. Noncompliance (Black-Hat Testing)

Noncompliance or black-hat testing is a specialized form of performance testing. Black-hat testing consists of the test team attempting to achieve the test goals (for example, penetration of a computer system) without being detected by any of the regular operating personnel or any of the system security features. Black-hat testing must be carefully coordinated because of safety and other concerns, such as adverse publicity.

Normal performance testing is the preferred mode of testing. However, black-hat testing may be the only method to assess the strength of all security features and procedures in the system. Typically, a black-hat test begins with assembling team members who have expertise in some part of the system being attacked. The team is then given a goal, such as penetration of a particular system to extract information. The team may be given information that is commonly available or may be asked to proceed without any special aid and develop its own information. The test team may coordinate with selected site personnel to ensure the continued protection of classified information and immediate detection of any vulnerabilities identified by the team.

Once the team has been successful in achieving its goals or the previously determined test period has elapsed, a debriefing occurs between the test team and the site personnel. During the debriefing the methods used by the test team are discussed and any weaknesses in security features or procedures are identified.

F. Review

The actual review begins with the request or decision to conduct a review. Once the protection criteria have been determined and the review techniques selected, the review team is responsible for using the techniques to collect information about the security posture of the systems and the functioning of the protection criteria. At regular intervals, perhaps daily, the review team should validate its findings and impressions with site personnel. The validation is necessary to prevent any incorrect or incomplete information from biasing the remaining activities of the team. The validation should be performed in a manner and location that permits an open and honest exchange of information between the site personnel and the review team.

G. Evaluation

After the review team has completed its planned activities and has accumulated enough information to permit it to assess the security status of the reviewed system, the team will organize its findings and present them to the proper site personnel. Depending upon the goals of the review, a verbal briefing may be appropriate. However, a written report outlining the team's findings and possibly recommendations for corrective actions is typically completed following the actual review. If a written review is prepared, a draft version of the report must be reviewed with the appropriate site personnel to confirm the report contents.

All notes collected during the review and any written reports should be treated as classified information until reviewed by a classification authority.

Once the review team has presented its outbriefing or the report, the site personnel must evaluate the findings and decide their response. The site may decide to implement corrective action or simply to accept the level of risk identified in the finding. In either case the site is expected to document their decision for use in later reviews.

Occasionally the review team may be contacted for additional information to help the site personnel understand a finding or to develop a solution. These requests typically do not require extensive interactions with or additional documentation from the review team.

VIII. APPLICATION OF REVIEW METHODOLOGY

Los Alamos has applied the methodology outlined in this paper to a typical computer system processing classified information in the DOE and developed a review checklist. The checklist contains questions directed towards protection criteria based on the security requirements and threats identified in orders and documents issued by the DOE Office of Safeguards and Security. The checklist does not include any oversight (Operations Office) or site specific requirements. The checklist provides only suggested items for incorporation in system specific criteria and is not intended to be a complete checklist for any computer system in the DOE. The checklist is available from the Safeguards Systems Group at Los Alamos.